CLAIMS

5

6

7

8

9

10

11

12

13

14

15

1. An authentication system suitable for automatically providing authentication to a user at a client node, the user providing a user secret and requesting access to network resources resident at one or more server nodes in a distributed network system, said authentication system comprising:

a local application program interface for receiving the user secret, said local application program interface in communication with a requested network resource;

a cryptography service node including means for providing a common key and algorithm, and means for providing a client/server session key and algorithm; and

an authentication database in communication with said local application program interface and with said cryptography service node, said authentication database including

an authentication secret associated with the user;

means for excrypting said authentication secret using said common key and algorithm; and

means for encrypting said common key using said client/server session key and algorithm.

- The authentication system of claim 1 further comprising means for encrypting and decrypting said authentication secret using a secret store key and algorithm.
- 1 3. The authentication system of claim 1 further comprising,
- a network resource identifier associated with said requested network
- resource; and
- a network policy associated with the user and with said network resource identifier.
- 1 4. The authentication system of claim 1 wherein said authentication database further comprises,

10

3	a second network resource identifier associated with a second network
4	resource;
5	a second authentication secret associated with the user; and
6	a second network policy associated with the user and with said second
7	network resource identifier.
1	5. The authentication system of claim 4 wherein said authentication database further
2	comprises means for encrypting and decrypting said second authentication secret using
3	said secret store key and algorithm.
	; ;
1	6. The authentication system of claim 4 wherein said authentication database further
2	comprises means for encrypting and decrypting said second authentication secret using a
3	second secret store key and algorithm.
1	7. The authentication system of claim 1 wherein said cryptography service further
2	comprises means for generating an authentication secret from the user secret.
1	8. The authentication system of claim 1 wherein said common key comprises a
2	symmetric key.
1	9. A method for automatically authenticating a user at a network client node in a
2	distributed network system in response to a user request for access to network resources
3	resident in one or more server hodes, said authentication method comprising the steps of:
4	providing a network resource identifier, a network resource policy, and an
5	authentication secret to an authentication database, said network resource
6	identifier associated with the requested network resource;
7	retrieving said authentication secret in response to said user request, said
8	authentication secret associated with the user and with said network resource
9	identifier;

encrypting said authentication secret with a common key and algorithm;

		/ '
11		encrypting said common key and algorithm with a dient/server session key and
12		algorithm; and
13		providing said encrypted authentication secret and said encrypted common key to
14		the client node.
1	10.	The method of claim 9 further comprising the steps of:
2		decrypting said encrypted common key using said client/server session key;
3		decrypting said encrypted authentication secret using said decrypted common key
4		and algorithm; and
5		providing said decrypted authentication secret to the requested network resource.
1	11.	The method of claim 9 further comprising the step of accessing said network
2	reso	arce policy prior to said step of retrieving said authentication secret, said network
3	reso	urce policy associated with the user and with said network resource identifier.
		//
1	12.	The method of claim 9 further comprising the steps of:
2		obtaining a list of client algorithms supported by the client node;
3		obtaining a list of server algorithms supported by the server node;
4		comparing said list of client algorithms with said list of server algorithms so as to
5		determine the strongest algorithm common to both said list of client
6		algorithms and said list of server algorithms; and
7		using said strongest algorithm as said common key and algorithm.
1	13.	The method of claim 9 wherein said common key comprises a symmetric key.
1	14.	The method of claim 9 further comprising the steps of:
2		negotiating the strongest common algorithm between server and client node; and
3	_	using said strongest algorithm as said client/server session key and algorithm.